Effective Date: 1/1/17

Configuration Management Standard

Purpose

The Configuration Management standard provides documentation of the minimum requirements for secure and compliant configuration of Division of Enterprise Technology (DET)/State IT systems and system environments.

Standard

Baseline secure and compliant IT system configurations must be based on one or more of the acceptable industry guidelines identified below. In addition, the latest vendor security guidance and DET IT Security Standards must be included in the configuration (CM-2).

Exceptions, changes or non-standard alterations to a secure and compliant configuration can be requested to meet a business or compliance need per the DET Exception Procedure.

Industry Guidelines

- Center for Internet Security (CIS) Benchmarks
- Defense Information Systems Agency (DISA) Standard Technical Implementation Guidelines (STIG)
- National Institute of Science and Technology (NIST) National Checklist Program
- United States Government Configuration Baselines (USGCB)
- National Security Agency Security Configuration Guides

Primary Regulatory and Compliance Requirements (for DET and/or its Agency customers)

- Centers for Medicare and Medicaid Services (CMS) - Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- Criminal Justice Information Services (CJIS) Security Policy
- Family Educational Rights and Privacy Act (FERPA) Compliance
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075
- Payment Card Industry – Data Security Standard (PCI-DSS)
- Social Security Administration (SSA) Technical System Security Requirements
- Wisconsin State Statutes Chapter 16.971

Effective Date: 1/1/17

Access

Physical and logical access to build, change, or maintain secure and compliant configurations must be limited to individuals with appropriate identified account types (e.g. privileged accounts) (AC-2, CM-5).

Environment

The initial setup, software installation, security configuration, and testing of new systems must be performed in a secure environment isolated from other operational systems with minimal communication protocols enabled (CM-2, CM-7).

An information system component inventory must be in place to accurately reflect current IT systems, applications, and components (CM-8).

Only identified DET/State owned and/or approved software can be installed on DET/State IT systems and system environments (CM-10).

Change management

Standard changes (i.e. updates) to secure and compliant configurations are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation in accordance with the DET Change Management Procedures (IT-715, DET Customer Manual) (CM-3). Individuals conducting security testing and impact analyses must possess the necessary skills and technical expertise to analyze the changes to information systems and the associated security ramifications (CM-2, CM-4). Exceptions, changes or non-standard alterations to a secure and compliant configuration can be requested to meet a business or compliance need per the DET Exception Procedure.

Records of changes and exceptions to secure and compliant baseline configurations must be retained for the life of the information system (CM-3).

Maintenance

DET must maintain configuration management plans that define detailed processes and procedures for how configuration management is used to support secure system development life cycle activities at the information system level (CM-9). Configuration management plans are typically developed during the development/acquisition phase of the secure system development life cycle.

Baseline secure and compliant configurations must be reviewed and updated:

- a minimum of annually;
- when required due to system upgrades, patches, or other significant changes; and
- as an integral part of information system component installations and upgrades (CM-2).

Effective Date: 1/1/17

Version	Approval/Revision/Review Date	Description	Approver/Author, Title
.1	4/27/2016	Original Draft	Jeff Thompson, Compliance Officer
.2	6/14/2016	Revisions and formatting	Tanya Choice, Cybersecurity Compliance Consultant
.3	8/9/2016	Draft finalized	DET Security, Audit and Compliance Team
1.0	11/22/16	Revisions and approval	Bill Nash Chief Information Security Officer

Authorized and Approved by:

Bill Nash Bill Nash 11/22/16

Print/Type Signature Date

Division of Enterprise Technology-Bureau of Security

Chief Information Security Officer

Effective Date: 1/1/17

Monitoring

A configuration monitoring process is in place to identify undiscovered or undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes (CM-6, CM-9). Information system scanning requirements are addressed in the Vulnerability Management Standard.

Definitions

- Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
- DET/State information - Any information that is created, accessed, used, stored, or transmitted by an Agency and/or DET.
- DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to; network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by DET.
- Identified Account Types include (AC-2): Individual, Privileged (Administrative and Default Privileged), Shared, Service, Emergency, and Temporary accounts.

Compliance References

IRS Pub. 1075
NIST 800-53 Revision 4

Exception Process

Exceptions to this and all DET Security policies or procedures must follow the DET Exception Procedures.

Document History/Owner

This standard was developed as required by the Department of Administration, DET Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, updates, and review of this document annually before the anniversary of the effective date.